## COMMENT

22 claims presented. Claims 1, 7, 10, 12 , 14, 16, 18, 20, 21, 22 are independent.

Claims 2, 4-6 depends directly or indirectly on independent claim 1.

Claims 8, 9 depend directly on independent claim 7.

Claim 11 depends directly on independent claim 10.

Claims 3, 13, 17 depend directly on independent claim 12.

Claim 15 depends directly on independent claim 14.

Independent claims 1, 7, 10, 14 require existence of identity system or information or program code or system "capable of being used in enabling electronic commerce operation(s)", whereas independent claim 12 require "identity software/means for providing second information(=identity information in other claims)" to obtain a "discouraging effect" for discouraging a user from enabling other user to use the software desired to be protected.

It should be noted although not explicitly indicated in the that claims 1, 10, 14, it should be understood therefrom that the identity information as claimed or the identity system as claimed is capable of being used to generate information which being information can be actually used to be authenticated by an electronic transaction apparatus trusted by a counterpart involved in the electronic commerce or a trusted party such as a clearing house, for causing an electronic commerce operation a rightful user has to be responsible for.

Such information should be highly confidential and be known only to its rightful user and the electronic transaction apparatus. Therefore, the identity information or the generated information as well as the identity system is well defined and it cannot be met by any existing information/system not being specifically made for the purpose of enabling electronic commerce operation(s).

Pls note that Claim 10 corresponding to the third embodiment as readable on original description, sheet 10, second and third paragraphs.

Independent claims 16, 18, 20 , recite a step (b), (c), (a) respectively, for **recognising a processing device**, in the present of an identity information or system and **thereafter, permitting use of software desired to be protected thereon**. This is another innovative feature of the present invention not being suggested or disclosed by

the cited prior art references Haas et al & the 2 Wiedemer patents, either considered individually or in combination.

Particularly, Claim 16 recites "obtaining from a user first information" and it has to be consistent with third information necessary for enabling electronic transaction(s) for which a rightful user of the software desired to be protected has to be responsible; and the method is being performed **without causing a said transaction take place** .

Claim 18, in particular, recites a sub-method for **verifying an account of a user being valid**, to obtain the "discouraging effect". Claim 18 further recites the sub-method recognises a processing device, for a cost from that user . It is clearly understood that the cost is for the use of the protected software on that recognised processing device by that user, because thereafter no further charge therefor, as readable on step (e).

Independent claims 18 further recites, thereafter, the sub-method capable of being used be used for **recognising another processing device, without re-charging the cost.**

Thus, a user who has paid for the protected software, can use the same on any processing device he desires or on the original processing device even after changes in software/hardware, without being fully re-charged, by using a discouraging effect to assure the software vendor that the protected software will continue to be used by that user.

Claim 20 recites "the presence of identity information/system in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform ... step (a)". This actually means that the protection software either determines the presence of identity information/system, like claim 1, or being combined with the identity program code in a non-separable manner, like claim 7. Further, claim 20 recites a sub-method after **recognising a processing device, capable of being used for recognising another processing device, without causing any user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor.**

## Argument for overcoming 103(a) rejections

## (Based on Haas et al. & 2 Wiedemer Patent)

In the Examiner's advisory action dated Sept 30, 2002, the Examiner admits that "Haas et al. qualifies as prior art under 102(e)" and does not oppose to my statement "only the patented invention should be included into prior art, excluding the description" as submitted in my argument "Argument for overcoming Haas et al.", first paragraph. Accordingly, I understand this as the Examiner's intimation of correctness of my statement.

Should the Examiner disagree, the Examiner is respectfully requested to indicate clearly in the next office communication.

As submitted in the previous argument, "Even though it is readable **on the description**, column 5, lines 47-54, Haas et al. teach a deterrent as causing by a software, a rightful user's credit card number to be displayed, to discourage a rightful user from sharing the software which being for decrypting a commercial software product, to other people. **This is not readable on the claims.**" For reasons as mentioned above, it should not be included into prior art to reject the present claims

The present invention as defined by the independent claims 1, 7, 10, 12 , 14, 16, 18, 20 (except claim 21 which control access to a processing apparatus) require existence of "identity system/information/software/program capable of being used in enabling electronic commerce operation(s)" as a precondition for providing user access to software desired to be protected, without causing an electronic commerce operation being performed. It can undoubtedly discourage a rightful user from sharing his software to an unauthorised user.

In the 2 Wiedemer Patents, they merely disclosed a security module 16 is being used for billing operation. And, as the Examiner has admitted in the Final Office action, P.6, section 13, and P.7 section 14, both second paragraph, in his arguments in support of 103 rejection of claims 1, 2, 4, 14, 15 and 17-22 and another 103 rejection

of claims 12, 13, 16 rspectively, "The Wiedemer/second Wiedemer patent does not disclose the step of not causing ..electronic commerce operation to be performed", while providing software protection.

It is respectfully submitted that, it is impossible for one with ordinary skill in the art to modify Wiedemer's billing module which most important purpose is to charge a user for usage of software, to not charge the user, so as to meet the requirement of the present independent claims 1, 7, 10, 12 , 14, 16, 18, 20, that is, "providing user access to software desired to be protected, without causing an electronic commerce operation being performed".

Also, for reasons as submitted here in above, this deficiency of Wiedemer cannot be supplied by Haas et al under 102(e).

Accordingly, the Examiner is respectfully requested to withdraw the two 35 USC 103 (a) rejections of the present independent claims 1, 7, 10, 12 , 14, 16, 18, 20 relying on Haas et al and the 2 Wiedemer patents.

Regarding claim 21, it is respectfully submitted that, it is an innovative feature of the present invention as defined by independent claim 21 that validity of a user account should be checked, without causing payment be made for access to paid protected software or a processing apparatus respectively, before providing user the access, and this is not being taught by the whole document of Haas et al. and the 2 Wiedemer patents, either consider individually or in combination.

Throughout Haas et al. document, there is no suggestion that validity of a user account should be checked, without causing payment be made for access to paid protected software. Haas et al. document merely teach in col.3, lines 53- 58, "user i transmits his ..credit card number(or billing purposes)".

Accordingly, 103(c) rejection of claim 21 basing on Haas et al. and Wiedemer should be withdrawn and is respectfully requested.

-1(Dirty)-

1. (Seven Times Amendment) A method for protecting software from unauthorised use, comprising the steps of:

determining if identity [means] system/information, is existing in a processing apparatus under control of a user ;

using [a favourable result of said determination] said identity system/information being determined as existing as a pre-condition for causing said processing apparatus to provide said user access to said software desired to be protected ;

wherein :

said identity [means] system/information, if so existing, being capable of being used in enabling electronic commerce operation(s) [for which rightful user(s) of said software desired to be protected has to be responsible] ;

access to said software desired to be protected is being provided without causing a said operation being performed and said identity [means] system/information being specific to [said] rightful user(s) of said software desired to be protected [and said software desired to be protected being licensed to said rightful user(s)] .

2. (Third Times Amendment) A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

authenticating said identity [means] system/information ;

determining said identity [means] system/information as existing, if [the result of] said identity system/information being determined as authentic [authentication is favourable] and as not existing if otherwise .

3. (Fifth Times Amendment) A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;

and for providing user access to third software if said computer being determined as authentic [authentication result is favourable] .

4. (Second Times Amendment) A method for protecting software from unauthorised use , as claimed in claim 1, wherein said operation being operation related to making payment from an account of said rightful user(s) , for obtaining a service/product.

6. (Third Times Amendment) A method for protecting software from unauthorised use, as claimed in claim 5, wherein further comprising the steps of:

[said processing apparatus having] storing an encrypted identity of [its rightful] a user in said processing apparatus ; and if [one] all of said protected programs stored in said processing apparatus has a valid user identity which being [not] consistent with the decryption result of said stored encrypted identity [of said processing apparatus], permitting use of said protected programs [will not be permitted] and [will be permitted] not permitting if otherwise .

7. (Sixth Times Amendment) A computer software product for protecting software publicly distributed against unauthorised use ;

said software product comprising :

identity program code for enabling electronic commerce operation(s) [for which rightful user(s) of said software desired to be protected has to be responsible] ;

authorising software [effectively under the control of said rightful user(s)] for, when executed, providing user access to said software desired to be protected, without causing a said operation being performed ;

a computer readable medium storing said identity program code and said authorising software ;

wherein :

said identity program code and said authorising software are [contained] stored in said [software product] medium in such a manner that said authorising software is prevented from being copied therefrom individually; and

the improvement resides in said protection basing on no specific hardware and/or software [specific to said rightful user(s)] other than said identity program code and said identity program code being specific to [said] rightful user(s) of said software desired to be protected ;

[and said identity program code and said authorising software existing in a computer readable medium] .

9. (Third Times Amendment) A computer software product as claimed in claim 7, wherein said authorising software contains said identity program code therein and said computer readable medium being in form of data signal embodied in a carrier wave.

10. (Eighth Times Amendment) A computer software product for protecting other software against unauthorised use , comprising :

authorising program for, when being executed, causing a processing apparatus to provide [providing] user access to said software desired to be protected ;

a computer readable medium storing said authorising program ;

wherein :

information specific to rightful user(s) of said software desired to be protected, exists in said authorising program as a part thereof ;

said existing information being capable of being used in enabling electronic commerce operation(s) [for which said rightful user(s) has to be responsible], but not being usable by said processing apparatus for said electronic commerce purpose, when said authorising program being loaded on said processing apparatus as a part thereof, and access to said software desired to be protected is being provided without causing a said operation being performed ;

[ said authorising program existing in a computer readable medium ].

11. (Third Times Amendment) A computer software product as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user(s) and said computer readable medium being in form of data signal embodied in a carrier wave.

-5(Dirty)-

12. (Seven Times Amendment) A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing apparatus having an identity software/means therein;

using said first information received being correct as a pre-condition for causing said processing apparatus to provide said user access to said software desired to be protected;

wherein:

said identity software/means being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ;

and said second information being capable of being used in enabling electronic commerce operation(s) [for which said rightful user(s) has to be responsible] ;

access to said software desired to be protected is being provided without causing a said operation being performed.

14. (Seven Times Amendment) A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/[means] system associated with a processing apparatus under control of a user ;

using [a favourable result of said authentication] said identity information/ system being determined as authentic as a pre-condition for causing said processing apparatus to provide said user access to said software desired to be protected ;

wherein said identity information/[means] system existing in such a manner that said identity information/[means] system being capable of being used in enabling electronic commerce operation(s) [for which rightful user(s) of said software desired to be protected has to be responsible] ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/[means] system being specific to [said] rightful user(s) of said software desired to be protected [and said software desired to be protected being licensed to said rightful user(s)].

16. (Seven Times Amendment) A method for protecting software from unauthorised use , comprising the steps of :

(a) obtaining by protection software running on a processing apparatus, say, first processing apparatus, first information from the user thereof ;

(b) determining by said protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with third information contained in said protection software ; thereafter

(c) authenticating a processing apparatus, say, second processing apparatus , basing on at least a part of said second information ;

(d) using [a favourable result of said authentication] said second processing apparatus being determined as authentic as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

wherein said third information being confidential information of a rightful user of said software desire to be protected and being necessary for enabling electronic transaction(s) for which said rightful user has to be responsible ; and said method is being performed without causing a said transaction take place .

-7(Dirty)-

18. (Seven Times Amendment) A method for protecting software from unauthorised use, by restricting the use thereof to be under control of a single person, comprising a sub-method ; said sub-method comprising the steps of :

(a) establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b) verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being [obtained] communicated to said remote electronic transaction system from said processing apparatus ;

(c) using [a favourable result of said verification] a valid account being verified as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter

(d) authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;

(e) using [a favourable result of said authentication] said second processing apparatus being determined as authentic as a pre-condition for permitting use of said software on said second processing apparatus, with no charge ;

wherein said sub-method a cost is being charged from said account ; and thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus , without re-charging from said account said cost .

19. (Third Times Amendment) A method for protecting software from unauthorised use, as claimed by claim 18, wherein no charge [by said software distribution system] for repeating [at least] said sub-method [steps c] to e)] .

20. (Seven Times Amendment) A method for protecting software, publicly distributed through a communications network, for use by a user, from unauthorised use ; comprising a sub-method ;

wherein said sub-method a protection software being used and "the presence of identity information/[means] system in a processing apparatus" is being used in the creation of said protection software as a pre-condition for said protection software to perform in said processing apparatus step (a) below ; and said identity information/[means] system being specific to said user and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

said sub-method comprising the steps of :

(a) determining by said protection software running on a processing apparatus, say, first processing apparatus with said precondition being met, first information related to the hardware or/and software of said first processing apparatus, for future reference in step (c) below ; thereafter

(b) determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof;

(c) determining if said second information is consistent with said first information ;

(d) using [a favourable result of said determination of consistence] said two information being determined as coinsistence as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing any user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor .

21. (Fourth Times Amendment) A method for verifying identity of a user of a data processing apparatus, comprising the steps of :

[a)] receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;

[b)] verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;

[c)] using by said data processing apparatus, [a favourable result of said verification] <u>said account validity being verified</u> as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said [steps a) to c) are] <u>method is</u> being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.

22. (Second Times Amendment) A software product comprising computer code for causing one or more processing apparatus to perform the method of claim 1, 12, 14, 16, 18 , 20 or 21 ;

[said computer code existing in] a computer readable medium storing said computer code.